clearswift
A HelpSystems Company

GUIDE *(Cybersecurity)*

Data Security: Controlling Classified Information in the UK Public Sector

Serious data breaches have a powerful effect on driving regulatory change and activity. Governments have always had secrets. But keeping secrets secret, and private information private, is proving a challenge for the public sector and government organizations have not been immune from large-scale incidents resulting in the exposure of millions of data records.

Government protective markings or classification systems are designed to help determine, and indicate to others, the levels of protection required to prevent the compromise of valuable or sensitive information. The markings signal quickly and unambiguously, the value of data and the level of protection it requires.

In this guide, we examine the UK classification policy and look at how data classification and data loss prevention software can help secure sensitive data in the public sector.

The UK Government Security Classifications Policy

In the UK, there is a system used to protect information from intentional or inadvertent release to unauthorized users. The system is organized by the Cabinet Office and is implemented throughout central and local government and critical national infrastructure. The system is also used by private sector bodies that provide services to the public sector.

The current classification system, the Government Security Classifications Policy (GSCP), replaced the old Government Protective Marking Scheme in 2014. Since classifications can last for 100 years, many documents written using the old scheme still exist and need protection.

Classifications must be capitalized and centrally noted at the top and bottom of each document page, except at OFFICIAL, where the document marking is optional. All material produced by a public body in the UK must be presumed to be OFFICIAL unless it is otherwise marked. Like the Protective Marking Scheme which it superseded, the GSCP classifications are applied only to the confidentiality of the data under classification.

TOP SECRET – Information is marked TOP SECRET if its release is liable to cause considerable loss of life, international diplomatic incidents, or severely impact ongoing intelligence operations. Disclosure of such information is assumed to be above the threshold for Official Secrets Act prosecution.

SECRET – This marking is used for information which needs protection against serious threats, and which could cause serious harm if compromised – such as threats to life, compromising major crime investigations, or harming international relations.

OFFICIAL – All routine public sector business, operations and services is treated as OFFICIAL. Many departments and agencies operate exclusively at this level.

The older protective marking scheme used five levels of classification, supplemented with caveat keywords. In descending order of secrecy, these were: Top Secret, Secret, Confidential, Restricted and Protect. The terms "UNCLASSIFIED" or "NOT PROTECTIVELY MARKED" were also used to indicate positively that a protective marking is not needed. Documents classified under the Government Protective Marking Scheme still exist and need correct handling.

Consistent use of protective markings or classifications, coupled with the adoption of appropriate security measures, enhances government's ability to conduct business in a secure and effective manner. Classifications/protective markings act as an important visual signal to anyone accessing or using the material, informing the minimum security obligations that need to accompany public sector data. They offer an easily identifiable way for information users (visually) and for downstream security tools (such as an entity's email or web gateway) to identify and manage the handling and control of information at different levels.

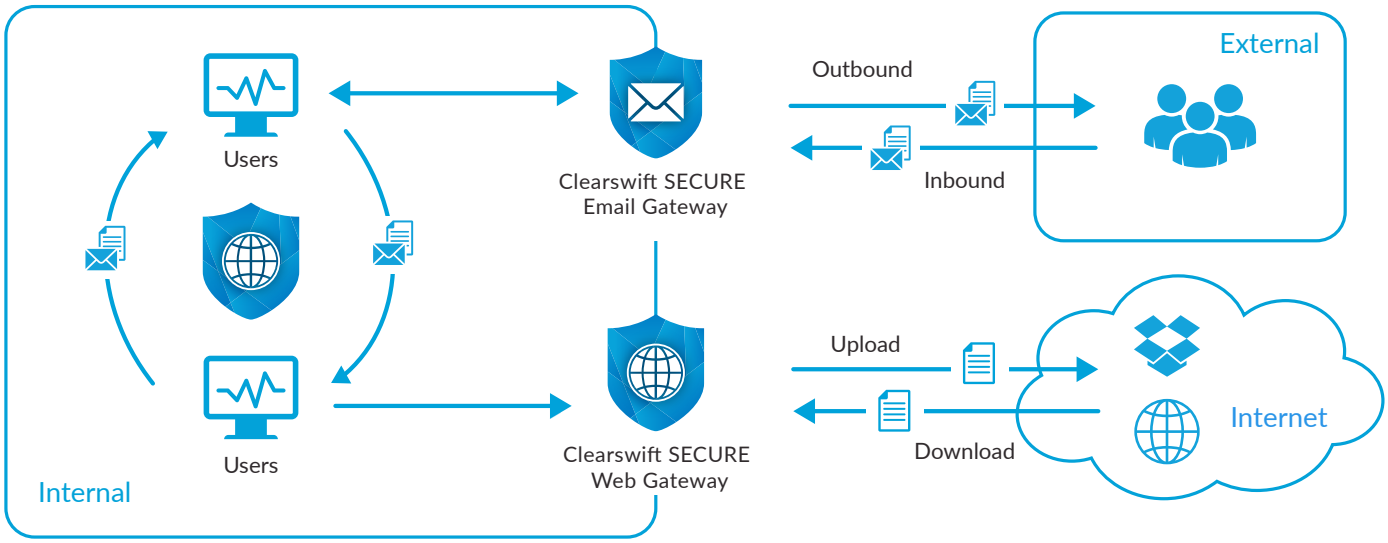
Data-centric Security

Clearswift has a long history of working with UK government organizations helping them to minimize data loss risks. Its adaptive data loss prevention (DLP) solution secures business communication channels ensuring that data is handled correctly in accordance with its classification.

Working alongside best-of-breed classification tools from Boldon James and Titus, Clearswift provides a combined DLP and data classification solution that is both easy to use and secure.

DLP and Data Classification Working Together

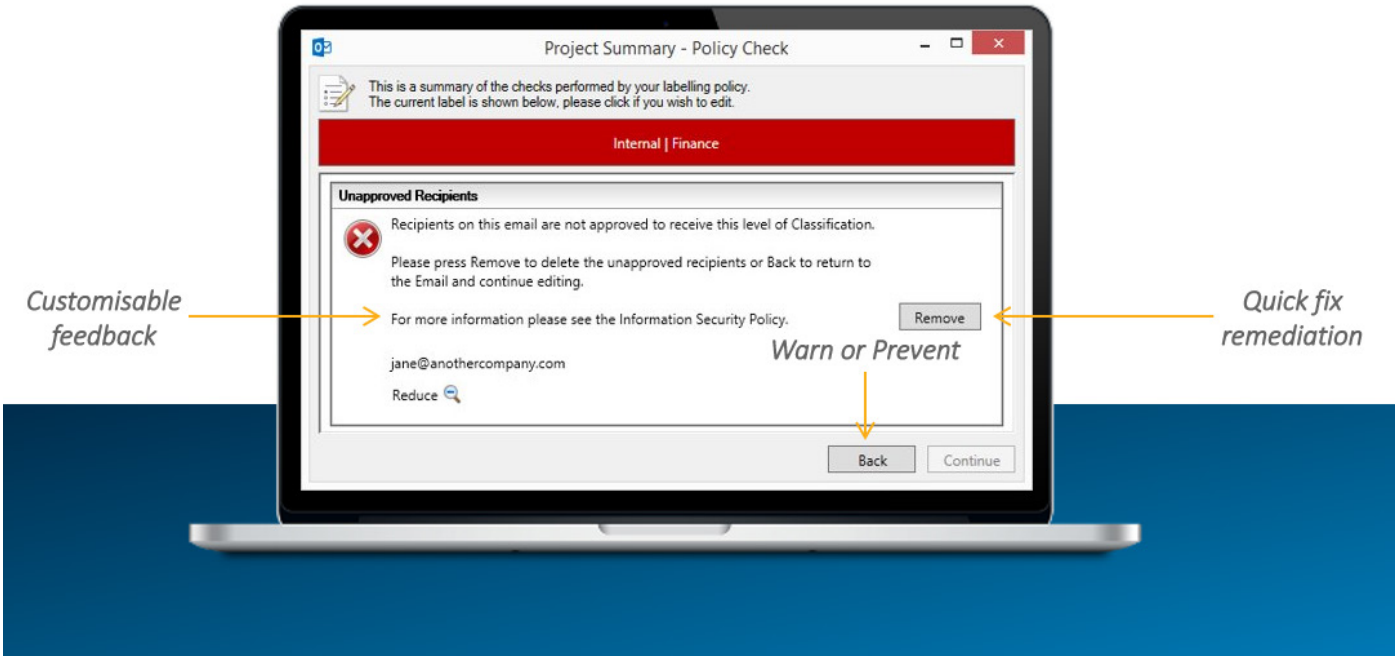
The Clearswift Secure Email, Exchange, and Web Gateways automatically enforce data classification policies for marked emails and documents. The policies can be applied to internal and external mail and uploads or downloads from the web (webmail, OneDrive, Dropbox etc).



Central to all Clearswift solutions is a Deep Content Inspection (DCI) engine that inspects data and applies the appropriate security policy. The solution checks the classification markings in the email or attached document and looks at the metadata, such as document properties and revision history. This ensures that data is processed in accordance with its classification. The level of classification also dictates the encryption policy the solution applies.

> ***"The depth and granularity provided by Clearswift's unique Deep Content Inspection engine provides customers with greater assurance that classified information is being treated correctly. Customers find it delivers a depth of protection for a broader range of formats than that provided by Microsoft 365 and Azure Information Protection."***
>
> **Alyn Hockey, VP Product Management.**

For example, the DCI engine looks for a TOP SECRET marking on an email or document and ensures that recipients are authorized to receive it before encrypting the data and sending it securely over TLS. If the receiver is not authorized, the sender is notified.



Flexible and Granular Policy Controls

New documents, spreadsheets, or presentations are sometimes created from existing files. This creates a risk that a highly classified document is modified and reclassified at a lower level without the original information being removed from its history.

Clearswift's DCI engine inspects the hidden metadata and applies the appropriate classification policy or redacts the document history, removing the previously classified information and ensuring compliance. Other policy actions can include blocking, notifying an end user or manager and encryption.

In addition to classification-based policies, the Secure Gateways can also apply policies based on user-specified rules for Personally Identifiable Information (PII), or user-specified structured data such as customer numbers or intellectual property markers.

Advanced features including Optical Character Recognition (OCR) and Anti-Steganography technology allow for images and scanned documents to be inspected and sanitized, ensuring that the risk of data loss through these files types is also minimized.

Additional Hygiene Features

Clearswift's Secure Email and Web Gateways provide standard hygiene protection including anti-spam controls, anti-virus options and can identify and control certain file types, for example, executable or script files embedded within compressed file formats. Clearswift's unique Structural Sanitization feature removes active content from emails or documents, protecting against advance threats that traditional anti-virus or sandbox technologies cannot detect.

Summary

It is essential that government organizations and the private sector bodies in their supply chain have the right solutions in place to minimize the risk of data loss in the public sector. Systems for data classification and data loss prevention allow organizations to effectively control and manage data and ensure compliance with industry regulations.

Clearswift DLP, integrated with Boldon James or Titus data classification systems, provides seamless enforcement of classification policies, ensuring that data is handled correctly when transmitted by email or over the web to keep it safe and compliant.

Clearswift, Boldon James, and Titus are all part of HelpSystems' Data Security suite.

For more information on our combined solution, visit www.clearswift.com/products/data-security-products.

clearswift
A HelpSystems Company
www.clearswift.com